The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/17/2020

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in iOS, iPadOS, watchOS, tvOS, watchOS, Xcode, and Safari. The most severe of these vulnerabilities could allow for arbitrary code execution.

- iOS is a mobile operating system for Apple cellphones.
- iPadOS is a mobile operating system for Apple tablets.
- tvOS is an operating system for the Apple media streaming device Apple TV.
- WatchOS is an operating system for Apple watches.
- Safari is a web browser available for macOS.
- Xcode is an integrated development environment (IDE) for macOS.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- iOS prior to 14.0
- iPadOS prior to 14.0
- watchOS prior to 7.0
- tvOS prior to 14.0
- Xcode prior to 12.0
- Safari prior to 14.0

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in iOS, iPadOS, watchOS, tvOS, Safari, and Xcode. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A lock screen issue allowed access to messages on a locked device. This issue was addressed with improved state management. (CVE-2020-9959)
- A logic issue was addressed with improved restrictions. (CVE-2020-9968)
- A logic issue was addressed with improved state management. (CVE-2020-9976)
- A memory initialization issue was addressed with improved memory handling. (CVE-2020-9964)
- An input validation issue was addressed with improved input validation. (CVE-2020-9952)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2020-9973)
- An out-of-bounds write issues were addressed with improved bounds checking. (CVE-2020-9958, CVE-2020-9983)
- A trust issue was addressed by removing a legacy API. (CVE-2020-9979)
- A type confusion issue was addressed with improved memory handling. (CVE-2020-9948)
- A use after free issue was addressed with improved memory management. (CVE-2020-9951)
- The issue was addressed with improved handling of icon caches. (CVE-2020-9773)
- This issue was addressed by encrypting communications over the network to devices running iOS 14, iPadOS 14, tvOS 14, and watchOS 7. (CVE-2020-9992)
- This issue was addressed with improved checks. (CVE-2020-9946)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Successful exploitation of these vulnerabilities could allow the attacker to execute remote code on the affected system.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.

- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT211843
https://support.apple.com/en-us/HT211844
https://support.apple.com/en-us/HT211845
https://support.apple.com/en-us/HT211848
https://support.apple.com/en-us/HT211850

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9773
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9946
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9948
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9951
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9952
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9958
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9959
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9964
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9968
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9973
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9976
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9979
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9983
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9992